REMARKS

1. Applicant thanks the Examiner for the Examiner's comments, which have greatly assisted Applicant in responding.

2. **Information Disclosure Statement**. The Examiner stated that the references in the Specification is not a proper information disclosure statement, and that unless the references have been cited by the Examiner on form PTO-892, they have not been considered.

Applicant has attached hereto an Information Disclosure Statement including references cited in the Specification.

Applicant is of the opinion that such IDS is complete.

3. **35 U.S.C. §103(a)**. The Examiner has rejected Claims 1-23 as being unpatentable over Gopinathan *et al* 5,819,226 (Gopinathan) in view of Sheppard 6,026,397. Applicant respectfully disagrees.

Claim 1-19

Independent Claim 1 appears as follows (emphasis added):

1. A computer implemented method of processing a transaction to determine the risk of transaction, the method comprising:

storing a plurality of merchant clusters, **the merchant clusters determined from statistical co-occurrences of the merchant names in a plurality of transactions**;

receiving data from a transaction between a consumer and merchant;

determining one of the plurality of merchant clusters associated with the merchant of the transaction based on the merchant's name; and

applying the merchant cluster in conjunction with data derived from the transaction to a predictive model to determine a level of risk of the transaction.

Specifically, the Examiner stated that Gopinathan shows a computer process to determine risk of a transaction receiving data from a transaction between a customer and merchant; determine which cluster associates (SIC code & Factor Group) with the merchant's name in the transaction ... and cites Col. 1, lines 27-42; Claims 2, 7, and 9.

Nowhere does Gopinathan or Sheppard teach or contemplate alone or in combination 'determine which cluster associates with the merchant's name in the transaction'. In contrast, such cited sections discuss transferring customer data from a former account to a new account on receiving a report that the customer's card has been lost or stolen; a database containing general customer data and a database containing customer transactional pattern data; generating a signal indicative of likelihood of fraud based on applying current transactional data and customer data to a predictive method; and a fraud detection rate measurement and a false positive rate measurement. Indeed, the document as a whole does not teach or contemplate 'determine which cluster associates with the merchant's name in the transaction'.

Claims 20-23

Independent Claim 20 appears as follows (emphasis added):

> 20. A method of determining a level of risk in a transaction, the method comprising:
>
> receiving a transaction between a first entity and a second entity;
>
> deriving high categorical information elements from at least one of transaction, the first entity or the second entity;
>
> **determining a low categorical information cluster closest to the high categorical information elements;**
>
> applying the low categorical information cluster and data derived from the transaction to a predictive model to determine the level of risk in the transaction.

The Examiner stated that it would have been obvious to include merchant name clustering and segmenting of the merchant names into data to supplement a predictive model in order to gain clarity over the SIC factors because it does not capture

segmentation details (transaction statistics) that would improve the ability to detect fraud in the model of Gopinathan and thus the risk involved with particular merchants in a particular segmentation as better defined that the SIC codes.

However, nowhere do Gopinathan and Sheppard teach or contemplate alone or in combination 'determining a low categorical information cluster closet to the high categorical information elements'.

Therefore, in view of the above, Applicant is of the opinion that Claims 1-23 overcome the Examiner's rejections. Hence, Applicant is of the opinion that Claims 1-23 are in condition for allowance. Accordingly, Applicant respectfully requests that the Examiner withdraw the rejection under 35 U.S.C. §103(a).

4. Applicant has amended Claims 15-17 to depend correctly on Claim 14, as opposed to Claim 6, which was done inadvertently. Support is found in the Claims, themselves, citing, "wherein determining the affinity measure of ... ."

It should be appreciated that Applicant has elected to amend Claims 15-17 solely for the purpose of expediting the patent application process in a manner consistent with the PTO's Patent Business Goals, 65 Fed. Reg. 54603 (9/8/00). In making such amendment, Applicant has not and does not in any way narrow the scope of protection to which Applicant considers the invention herein to be entitled. Rather, Applicant reserves Applicant's right to pursue such protection at a later point in time and merely seeks to pursue protection for the subject matter presented in this submission.

CONCLUSION

Based on the foregoing, Applicant considers the present invention to be distinguished from the art of record. Accordingly, Applicant earnestly solicits the Examiner's withdrawal of the rejections raised in the above referenced Office Action, such that a Notice of Allowance is forwarded to Applicant, and the present application is therefore allowed to issue as a United States patent. The Examiner is invited to call to discuss the response.

Respectfully Submitted,

Michael A. Glenn
Reg. No. 30,176

Customer No. 22862

Amendment to the Claims

We claim:

1. (original) A computer implemented method of processing a transaction to determine the risk of transaction, the method comprising:

storing a plurality of merchant clusters, the merchant clusters determined from statistical co-occurrences of the merchant names in a plurality of transactions;

receiving data from a transaction between a consumer and merchant;

determining one of the plurality of merchant clusters associated with the merchant of the transaction based on the merchant's name; and

applying the merchant cluster in conjunction with data derived from the transaction to a predictive model to determine a level of risk of the transaction.

2. (original) The method of claim 1, further comprising:
estimating a likelihood that the transaction is fraudulent.

3. (original) The method of claim 1, responsive to the level of risk of the transaction, determining whether to approve the transaction, decline the transaction, or obtain additional information regarding the transaction or the cardholder.

4. (original) The method of claim 1, wherein determining one of the plurality of merchant clusters associated with the merchant further comprises:

storing a lookup table associating each merchant cluster with at least one merchant name, wherein the merchant names are each unique;

applying the merchant's name to the lookup table to determine the associated merchant cluster.

5. (original) The method of claim 4, wherein the unique merchant names are derived from a plurality of raw merchant names in transaction data by stemming and equivalencing the raw merchant names.

6. (original) The method of claim 1, further comprising:

storing for each merchant cluster a risk factor indicative of the likelihood that transactions at merchants within the merchant cluster are fraudulent; and

applying the risk factor of the merchant cluster to the predictive model.

7. (original) The method of claim 6, wherein the risk factor is an estimate of the percentage of transactions in the merchant cluster that are fraudulent.

8. (original) The method of claim 1, further comprising:

storing a plurality of consumer clusters;

storing for each combination of a consumer cluster and a merchant cluster a risk factor indicative of the likelihood that transactions by consumers in the consumer cluster at merchants within the merchant cluster are fraudulent;

determining a current cardholder cluster associated with the cardholder; and

applying the risk factor of the combination of the current cardholder cluster and the merchant cluster to the predictive model.

9. (original) The method of claim 8, wherein the risk factor is an estimate of the percentage of transactions in the merchant cluster by consumers in the cardholder cluster that are fraudulent.

10. (original) The method of claim 1, further comprising:

storing for each merchant cluster at least one summarized transaction statistic, descriptive of transactions occurring at merchants in the merchant cluster; and

applying the at least one summarized transaction statistic of the merchant cluster to the predictive model.

11. (original) The method of claim 10, wherein the at least one summarized transaction statistic are selected from a group consisting of:

average transaction amount; and

average transaction volume.

12. (original) The method of claim 1, further comprising:

storing for each of a plurality of consumer clusters, at least one summarized transaction statistic, descriptive of transactions by consumers in the consumer cluster; and

applying the at least one summarized transaction statistic of the consumer cluster to the predictive model.

13. (original) The method of claim 10, wherein the at least one summarized transaction statistic are selected from a group consisting of:

average transaction amount; and

average transaction volume.

14. (original) A computer implemented method of processing a transaction to determine the risk of transaction, the method comprising:

storing a plurality of merchant clusters, the merchant clusters determined from statistical co-occurrences of the merchant names in a plurality of transactions;

receiving data of a transaction between a consumer and merchant;

determining one of the plurality of merchant clusters associated with the merchant of the transaction based on the merchant name;

determining an affinity measure of an affinity of cardholder to the merchant cluster; and

applying the affinity measure in conjunction with data derived from the transaction to a predictive model to determine the level of risk of the transaction.

15. (currently amended) The method of claim [[6]]14, wherein determining the affinity measure of an affinity of the cardholder to the merchant cluster further comprises:

determining an affinity vector of the affinity of the cardholder to each of a plurality of merchant clusters, including the merchant cluster of the merchant of the transaction.

16. (currently amended) The method of claim [[6]]14, wherein determining the affinity measure of an affinity of the cardholder to the merchant cluster further comprises:

determining a cardholder cluster associated with the cardholder; and

determining an affinity measure of the affinity of the cardholder cluster to the merchant cluster.

17. (currently amended) The method of claim [[6]]14, wherein determining the affinity measure of an affinity of the cardholder to the merchant cluster further comprises:

determining a cardholder cluster associated with the cardholder; and

determining an affinity vector of the affinity of the cardholder cluster to each of a plurality of merchant clusters, including the merchant cluster of the merchant of the transaction.

18. (original) A method of determining the level of risk in a transaction by consumer, the method comprising:

storing a plurality of merchant clusters, the merchant clusters determined from statistical co-occurrences of the merchant names in a plurality of transactions;

receiving data of a current transaction between a consumer and merchant;

determining a predicted merchant cluster in which the consumer is predicted to have a future transaction based on transactions of the consumer prior to the current transaction;

determining an actual merchant cluster associated with the merchant of the transaction based on the merchant name;

determining a difference measure between the predicted merchant cluster and the actual merchant cluster; and

applying the difference measure in conjunction with data derived from the transaction to a predictive model to determine the level of risk of the transaction.

19. (original) A system for detecting risk in a transaction, comprising:

a database of unique merchant names, each merchant name associated with a merchant cluster;

a transaction processing component that receives a transaction between a consumer and a merchant, that derives transaction data from the transaction, and determine a unique merchant name for the merchant from the database; and

a statistical model that receives the data derived from the transaction and the unique merchant name, and outputs a score indicative of the level of risk in a transaction.

20. (original) A method of determining a level of risk in a transaction, the method comprising:

receiving a transaction between a first entity and a second entity;

deriving high categorical information elements from at least one of transaction, the first entity or the second entity;

determining a low categorical information cluster closest to the high categorical information elements;

applying the low categorical information cluster and data derived from the transaction to a predictive model to determine the level of risk in the transaction.

21. (original) The method of claim 20, wherein the high categorical information elements are text data.

22. (original) The method of claim 20, wherein the second entity a merchant of the transaction, and the high categorical information elements are merchant notes associated with the transaction.

23. (original) The method of claim 20, further comprising:

selecting a plurality of high categorical information elements;

associating each high categorical information element with a context vector in a vector space, such that high categorical information elements that frequently proximally co-occur in the transactions have context vectors that are similarly oriented in the vector space;

clustering the context vectors of the high categorical information elements into a number of clusters substantially less than the number of high categorical information elements, each cluster being a low categorical information cluster;

wherein determining a low categorical information cluster closest to the high categorical information elements further comprises determining the low categorical information cluster closest in the vector space to a context vector derived from the context vectors of the high categorical information elements.